UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,321	03/02/2004	Christopher N. Kline	END920030127US1	1828

26502 7590 08/31/2007

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
08/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mn

Office Action Summary	Application No.	Applicant(s)	
	10/791,321	KLINE, CHRISTOPHER N.	
	Examiner	Art Unit	
	Amare F. Tabor	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/02/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 are examined.

Specification

2. The abstract of the disclosure is objected to because it contains more than 150 words. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3, 11, 16 and 17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 3, the limitation in claim 3 "***group name not on the list of group names generally used for a group with higher level privilege***" can be rephrased as "***group name on the list of group names generally used for a group with user level privilege,***" which is function of the third program instruction. (According to the disclosure of the application, privilege levels are grouped into two parts: "user" privilege level or some other higher privilege; see page 11, lines 20-21). Therefore, the examiner understands the functions of the third and fourth program instruction to be identical.

Regarding claim 11, the limitations in claim 11 recite similar limitations that are specified in claim 1. Therefore, the examiner treats claim 1 and 11 as a duplicate of claims.

Regarding claims 16 and 17, it is not clear how the function of the first program instruction has changed from "***first program instruction to compare members within each said group to list of trusted individuals***" to "***first program instructions to determine if any group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege or no privilege***" recited in claims 16 and 17. Similarly, it is not clear how the original function of the second program instruction, as recited in claim 1, has changed to the functions recited in claims 16 and 17.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sakushima et al. (US Pat No.: 7,103,777 B2), referred as "***Sakushima***" hereinafter, and further in view of "***Huang***" (US Pat No.: 6,192,361 B1).

5. *As per claims 1, 3 and 11,* Sakushima discloses,

A computer program product for determining if any of a plurality of groups may have an improper actual level of privilege, said computer program product comprising: a computer readable medium; (abstract, lines 1-13, "a user information management apparatus and method capable of efficiently preventing user information from being utilized by another person in family or being distributed to the outside, thereby protecting security; a recording medium having recorded therein a control program for managing user").

- first program instructions to compare access privilege level; (FIG.18 & column 16, lines 13-14 and 18-26, "the 'access' accepted by the access accepting section 182 used here denotes an instruction or command for applying processing to the data") and ("the access privilege determining section determines the presence or absence of access privilege for the data access accepted at the access accepting section 182. That is, an access privilege of an entity causing the access accepting section 182 to accept an access, or alternatively, an access privilege of the user information management apparatus 180 itself is compared with an access privilege data specified by access 181, and it is determined whether or not access to data by means of the access 181 is permitted").

- second program instructions to determine if actual privilege level is higher than user level privilege, (column 4, lines 14-17, "if a current certification level of the user is lower than a desired certification level required for data acquisition, instruct the user to take action required to level up to the required certification level") and (FIG.27 & column 18, lines 54-61, "at the step S271, it is determined whether or not data access privilege is too low. That is, it is determined whether or not the access level stored in the access management section 185 is lower than that of data to be accessed. If it is determined

that the access level is lower, processing goes to the step 272 and processing for increasing the access level that is access privilege is carried out. For example, certification for increasing access level is carried out").

- third program instructions to determine if actual privilege level higher than user level privilege has a user level privilege, (FIG.27 & column 18 line 62 through column 19 line 3, "when it is determined that the data access privilege is not too low at the step S271, processing goes to the step S273 at which the data access privilege is determined whether or not it is too high. That is, it is determined whether or not access cannot be made because the access level stored in the access management section 185 is higher than the access level required to access data. If so, processing goes to the step S274 at which access privilege obtained as an access level is lowered").

- said first, second and third instructions are recorded on said medium; (column 3, lines 30-35, "there is provided a recording medium having recorded therein in a computer readable state a control program for executing the user information management method in the user information management apparatus constructed over a server capable of making bidirectional communication with a user").

Sakushima does not explicitly disclose,

- generating a report identifying said at least one member not on the list of trusted individuals and the group in which said at least one member is a member;

However, in the same field of endeavor, Huang disclose:

- list of trusted individuals; (column 2, lines 8-10, "the full group privileges access mechanism of the present invention contains storage files which store information related to authorized users").

- members and user groups with privilege levels; (column 2, lines 61-65, "the full group privileges access mechanism of the present invention supports multiple user groups wherein the members of the respective user groups have varying degrees of access to the telecommunications switching system, as compared to members of other user groups).

- generating a report identifying member not on the list of trusted individuals; (see FIG. 3A and column 15, lines 15-27, "as shown in Block 88, System Manager 18, in conjunction with System Security Manager Client 54 and System Security Manager Sever 58, then access the records containing the list of valid User IDs and Passwords, which records are maintained in the System Manager Runtime Library 19, and compare the user's User ID and Password to the list of valid User IDs and Passwords. As shown in Blocks 90 and 92, if the Full Group Privileges Access Mechanism determines that the user's

User ID or Password is not valid, the Full Group Privileges Access Mechanism generates a record of the attempted unauthorized access, and transmits a Failed Logon message to Remote Computer 10, which in turn displays the message to the user").

- and generating a report that said group with the higher actual privilege level has a group name generally used for a group with user level privilege, such that the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are revealed as trusted or not trusted; (see FIG. 3B and column 16, lines 11-17, "as shown in Blocks 106 and 108, if the user is not authorized to execute the command or access the function, the Full Group Privileges Access Mechanism generates a record of the attempted unauthorized access, and sends a message to Remote Computer 10 indicating that the user's attempt to access the Telecommunications Switch Management System has failed).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teachings of Huang to the method of Sakushima, because one of ordinary skill in the art would want to ensure that the full privilege access mechanism serves only authorized users (see Huang column 11, lines 22-26).

6. *As per claim 2 and 12*, Sakushima discloses,

- third program instructions; (see rejection of claim 1 above).

Sakushima does not explicitly disclose,

- wherein there are a plurality of applications or application instances, and a same group can be assigned different privilege levels for involvement with different applications or application instances; and making determination separately for each application or application instance

However, Huang disclose the above limitation as, (see Table 2 in column 13 and column 2, lines 46-53, "the storage files store information related to user groups which have authorized users as members, and information related to the user groups which are authorized to access each function and execute each instruction provided by the telecommunications switching system. A user cannot access a function or execute a command unless the user is a member of at least one user group which is authorized to access that function or execute that command").

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teachings of Huang to the method of Sakushima, because one of ordinary skill in the art would want to provide a security system with increased flexibility and the ability to be customized (see Huang column 3, lines 14-19).

7. As per claim 4 and 13, Sakushima discloses,

- ***second program instruction*** (see rejection of claim 1 above).

Sakushima does not explicitly disclose,

- ***determining if any group with an actual privilege level higher than user level privilege have all of its members on the list of trusted individuals, and if so, generate a report that said group with the higher actual privilege level has all its members on the list of trusted individuals***

However, in the same field of endeavor, Huang disclose:

- ***list of trusted individuals; members and user groups with privilege levels; and generating a report;*** (see rejection of claim 1 above).
- ***determining if any group have all of its members on the list of trusted individuals;*** (column 11, lines 61-67, "when a user attempts to access the Telecommunications Switch Management System, the Full Group Privileges Access Mechanism compares the user's User ID and Password against its records of authorized User IDs, the expiration date and time for each authorized User ID, authorized Passwords for each authorized User ID, and the expiration date and time for each authorized Password. The Full Group Privileges Access Mechanism will refuse the user access to the Telecommunications Switch Management System unless the user has a valid and unexpired User ID and Password").

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teachings of Huang to the method of Sakushima, because one of ordinary skill in the art would want to ensure that a user cannot access any portion or function of the system which the user is not specifically authorized to access, even if a particular user is generally authorized to access the system (see Huang column 11, lines 26-30).

8. As per claim 5 and 14, Sakushima discloses,

- ***second program instruction; and computer readable medium;*** (see rejection of claim 1 above as applied to third program instruction).

Sakushima does not explicitly disclose,

- ***determining if all the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are on the list of trusted individuals;*** (see rejections of claim 4 above).

9. As per claims 6 and 8, rejection of claim 1 is incorporated.

A computer system for determining if any of a plurality of groups may have an improper actual level of privilege, said computer system comprising: (see rejection of claim 1 above).

Claims 6 and 8 are apparatus claims corresponding to the process of claim 1 and are rejected for the rejections of claim 1 include inherent means; and further Sakushima discloses,

- means for comparing members within each of said groups to a list of trusted individuals; (column 2, lines 55-57, "level determination means for, when the user makes access to the server, determining at which of a plurality of predetermined certification levels this access is").

- and means for determining if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals; and means for determining if any group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege; (column 2, lines 58-62, "transmission control means for enabling transmission of only the user information at the security level and the lower security level than said security level that corresponds to the determined level to the user terminal and/or another device among the user information held in the storage means").

- generate a report identifying said at least one member not on the list of trusted individuals and the group in which said at least one member is a member; (see rejection of claim 1).

- generate a report that said group with the higher actual privilege level has a group name generally used for a group with user level privilege, such that the members of said groups with the higher actual privilege having a group name generally used for a group with user level privilege are revealed as trusted or not trusted (see rejection of claim 1).

10. As per claim 7, rejection of claim 2 is incorporated.

Claim 7 is apparatus claim corresponding to the process of claim 2 and is rejected for the rejections of claim 2 include inherent means; and further Sakushima discloses,

- means for determining if any group with an actual privilege level higher than user level privilege has a group name generally used for a group with user level privilege makes its determination separately for each application or application instance; (column 2, lines 52-54, "identification means for, when a user makes access to the server and an attempt is made by the user to use a predetermined application, identifying the user).

- wherein there are a plurality of applications or application instances, and a same group can be assigned different privilege levels for involvement with different applications or application instances; (see rejection of claim 2).

11. *As per claim 9 and 10,* rejection of claim 4 is incorporated.

Claims 9 and 10 are apparatus claims corresponding to the process of claim 4 and is rejected for the rejections of claim 4 include inherent ***means for determining if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals determines if any group with an actual privilege level higher than user level privilege have all of its members on the list of trusted individuals;***

- and generates a report that said group with the higher actual privilege level has all its members on the list of trusted individuals (see rejection of claim 4).

12. *As per claim 15,* Sakushima discloses,

A computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; first program instructions to compare members within each of said groups to a list of trusted individuals; and second program instructions to determine if any groups with an actual privilege level higher than user level privilege have a member not on the list of trusted individuals (see rejection of claim 1).

- remove said member not on the list of trusted individuals from said group; (column 4, lines 42-46, "when the security division falls into a predetermined division among said security divisions, when a certification level is changed to be lowered, delete data transmitted from the server to the user terminal before the certification level is changed to be lowered") and (column 12, lines 48-55, "according to the security division when a change is made to a low security level due to timeout or logout, data transmitted to a user terminal is deleted. That is, when a predetermined security division is obtained, when a security level is lowered, data transmitted in a state in which a security level is high is automatically deleted, thereby preventing distribution or illegal use of such data").

13. *As per claims 16,* Sakushima discloses,

A computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; first program instructions to determine if any group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege or no privilege; and second

program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name generally used for a group with user level privilege or no privilege, to compare members of such group to a list of trusted individuals; (column 3, lines 43-48, "identification step of, when a user makes access to the server and an attempt is made by the user to use a predetermined application, identifying the user; and level determination step of, when the user makes access to the server, determining at which of a plurality of predetermined certification levels this access is").

- and if any member(s) of such group do not appear on said list of trusted individuals, remove said member(s) from such group that do not appear on the said list of trusted individuals; (column 12, lines 48-55, "according to the security division when a change is made to a low security level due to timeout or logout, data transmitted to a user terminal is deleted. That is, when a predetermined security division is obtained, when a security level is lowered, data transmitted in a state in which a security level is high is automatically deleted, thereby preventing distribution or illegal use of such data").

14. *As per claims 17,* rejection of claim 1 is incorporated and further Sakushima discloses,

A computer program product for managing privileges of groups, said computer program product comprising: a computer readable medium; first program instructions to determine if any group with an actual privilege level higher than user level privilege has a group name not on a list of group names generally used for a group with privilege level higher than user level privilege; and second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name not generally used for a group privilege level higher than user level privilege, to compare members of such group to a list of trusted individuals; (column 3, lines 43-45 and 49-53, "identification step of, when a user makes access to the server and an attempt is made by the user to use a predetermined application, identifying the user; and transmission control step of enabling transmission of only the user information at the security level and the lower security level than said security level that corresponds to the determined level to the user terminal and/or another device among the user information held in the storage step").

- list of trusted individuals; members and user groups with privilege levels; lowering actual privilege levels; (see rejections of claim 1).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare F. Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on (571) 272-3696. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AFT

JEAN M. CORRIELUS
PRIMARY EXAMINER
Art Unit 2162
Date: 8/30/07